Queen Elizabeth II High School

Acceptable Use Policy

gleck dty share dy kinjagh

Preamble

The purpose of this Policy is to provide a high level of e-safety for children, young people and staff using ICT whilst also facilitating a rich learning environment: it details the actions and behaviours that are required in order to maintain an e-safe environment.

This policy should be read in conjunction with DESC policy and guidelines for acceptable use, the QEII High School Communications Policy, the Mobile Phone Policy, the Policy and Procedures for dealing with sexting, relevant terms and conditions of work for employees and legislation such as GDPR.
Under-pinning the policy is the belief that users are most likely to remain e-safe when they are appropriately educated about the threats that IT the Internet and social media can pose.

Scope

The policy applies to all employees of DESC working at the School and to all students studying at the school.

Unacceptable Content

Unacceptable content is defined as: -Pornographic, adult, tasteless or offensive material; violence, racism, extremist or hatred views; illegal drug taking, criminal skills or software/media piracy,

Inappropriate Use

Inappropriate uses of IT include: -

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel

- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities
- Using AI tools and generative Chatbot's (such as ChatGPT and Google Gemini):
    - During assessments, including internal and external assessment and coursework
    - To write homework or classwork assignments, where AI-generated text or imagery is presented as their own work.
    - To produce content that is inappropriate, offensive, or harmful.
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher or any other relevant member of staff will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

Breach of this policy could lead to serious disciplinary action (gross misconduct/suspension) and possibly legal action.

Management of the network and hardware provided by GTS

GTS are responsible for the provision and maintenance of the computer network and internet access. This includes provision of relevant and appropriate screening and firewalls. Members of staff in school are required to work within the guidelines provided by GTS staff to ensure e-safety and security of documents and data.

Staff laptops are provided by GTS for professional use. Members of staff who are issued with a laptop are required to keep them safe, maintain secure passwords and ensure that personal data for students, parents and other staff is kept confidential and secure. If a laptop is lost or stolen, this must be reported immediately.

Teachers and support staff have a responsibility to remain vigilant and monitor use of electronic devices in school and to report any concerns to SLT and GTS staff. Safeguarding concerns for students should be logged using CPOMS. This includes reporting faults in equipment and possible misuse by students or other staff.

Mobile phones

Staff who use their own mobile phones for work purposes must ensure that any confidential data such as parental contact details are only held with permission of the person concerned. GTS issued mobile phones are subject to the same requirements as laptops.

Student use

Teachers have a responsibility to follow the Mobile Phone Policy. If the teacher allows students to use electronic devices in their lessons they must ensure that students are aware of the risks, know how to be safe and comply with this policy.

Students may bring their own devices into school but these must only be used for educational purposes with permission of the relevant teacher (see Mobile Phone policy). **Students MUST NOT make, share or store recordings (video or sound) or images of other people without their express permission.** Please see the schools Policy and Guidance document for dealing with incidents of "sexting'.

If students use their device inappropriately, either without permission or in breach of data protection or to access inappropriate materials, the device will be confiscated. In order to safeguard children, where deemed necessary, the Head Teacher or a member of staff acting on the authority of the Head Teacher can:

- Search and screen the device
- Instruct students to delete any inappropriate material.
- Confiscate and retain the device in the school safe for collection by a parent or carer

If any illegal content is discovered the school will consider contacting the police.

Confiscated devices may only be returned as per the Mobile Phone Policy or to a parent or carer. The student may then be banned from bringing such devices into school or be required to hand the device in to a member of staff on arrival to school.

Social media

Staff and students must be responsible when using social media. Deliberate downloading of unacceptable content, sharing of personal data or inappropriate use (see definitions above) will be treated as a disciplinary matter.

Social media may be used in line with the communications policy to share relevant information.

"Microsoft Teams" and "Google Docs" or "Google classroom" may be used to share teaching and learning materials.

Artificial Intelligence (AI)

In recognition of the rapid growth of artificial intelligence (AI) technologies and their potential to enhance educational experiences, Queen Elizabeth II High School is committed to facilitating the responsible and effective use of AI tools within our school and students may use AI tools and generative Chatbot's:

- As a research tool to help them find out about new topics and ideas
- When specifically studying and discussing AI in schoolwork, for example in IT lessons or art homework about AI-generated images. All AI-generated content must be properly attributed

For examples of prohibited use please see above.

This policy should be read in conjunction with the following policies and documents:

- Child Protection and Safeguarding
- Policy and Procedure for Dealing with Sexting
- Behaviour Policy
- Bullying Policy

Please refer to the additional guidance and information in Appendix A. Appendix B is the agreement form for students.

Appendix A Additional E-safety information and guidance for all

As well as the rules that you have agreed to obey there are also some extra guidelines that will help to keep you safe online:

- Be very careful when you get emails or messages from people who you do not know. If you get unknown messages or emails these should usually be deleted. If however they cause offence, then don't keep them to yourself. Report this to a member of staff/line manager.
- You should not meet anybody who you only know from the Internet or by email. People who send you messages on the Internet may not be who they say they are. Always share a request to meet.
- Remember that everything you do on the Internet leaves a "digital footprint". If you post a silly picture of yourself or of somebody else on the Internet then it may be copied, changed and sent to other people far beyond your control and for a long time into the future.
- If you are not sure if something is unacceptable or inappropriate for viewing or sharing in your school/college/youth project then here is some useful advice. If a parent or teacher/youth worker/line manager tells you that it is unacceptable or inappropriate then you must not view or share it. If you are unsure then seek advice.
- Be very careful about discussing any aspect of the school/college/youth project community on external websites as this may lead to accusations of inappropriate behaviour that could result in result in a disciplinary procedure.
- Be especially careful when using social networking apps or platforms such as Snapchat, Facebook, Instagram etc because these platforms make it easy for people to pretend to be somebody else. Most social networking sites have age restrictions. You should not access sites if you are under that age restriction. Always set your privacy settings so that only your friends can see your profile and your wall.
- Reporting abuse. Many websites will show the report abuse symbol that takes you to the CEOP site. You should familiarise yourself with the symbol and how to access help if you ever feel threatened online.

Appendix B ICT Acceptable Use Policy agreement for students

1. **These rules apply to all equipment.** I know that these rules will apply to me at all times when I am using either provided ICT equipment in school or at home, or my own ICT equipment within school, such as computers, cameras, phones, scanners, software and networks.
2. **Take care when using equipment.** I will take care when I am using all ICT equipment. I will not deliberately or recklessly break or damage any ICT equipment provided to me and if anything gets broken then I will report it straight away.
3. **Ask before using your own ICT equipment.** I will not bring my own ICT equipment with me unless I have been given permission by a designated member of staff. If I am allowed to bring my own ICT equipment then I will obey all the extra rules I will be given about how I can use it.
4. **Keep passwords safe.** I will always log on using my own user-name and password. I will not tell my login details to anybody else. I know that I will be responsible for everything that is done using my login details. If I think that somebody else knows and has used my login details then I will report it straight away so that my login details can be changed.
5. **Nothing is secret.** I realise that my use of both my own and provided ICT equipment will be monitored and that everything I do may be recorded whilst used on a Department network. I agree to being monitored and recorded at all times. I realise that the results of this monitoring may be shared with other people if I break any of the rules or if my actions are of a criminal nature.
6. **Keep personal information safe.** I will not disclose any of my personal details to other people, or display any personal details on websites. (Personal details include telephone numbers, addresses and all types of personal financial information.) I agree that I will never pass on the personal details of another person without that person's permission.
7. **Understanding copyright.** If I am downloading music, video or images, I will check with staff that it is legal and copyright free. I understand that music and video files are often put on the Internet illegally and that by using those files I will be breaking the law. I will not distribute works protected by intellectual property rights and will respect the rights, privacy and property of others.
8. **Educational uses only.** My use of ICT equipment will only be for educational uses, although limited personal use is permitted provided that this is not done during normal working time and does not contravene any of the other rules in this document.
9. **No hacking.** I will not try to access any websites, services, files or other resources that are blocked or which I am not allowed to try to access.

10. **Unacceptable or inappropriate material.** I agree that I will not try to view, send, upload or download material that is unacceptable or inappropriate for viewing. If I accidentally see any unacceptable or inappropriate material then I will immediately close (but not delete, in the case of emails) the material and tell a member of staff. I know I will not be held responsible if I view unacceptable or inappropriate material by accident and I realise that by reporting this I will help to improve the e-safety of my school/youth project. If I am in any doubt about the suitability of any material, or if any doubts are raised, then I will not (re)access the material. I will not access material that has been rated as unacceptable or inappropriate.
11. **Be polite.** Proper conduct and courtesy must be maintained at all times while using ICT as in any other form of communication. I agree that I will not harass, intimidate, bully, insult or attack others via email or any other means. The use of strong language, swearing or aggressive behaviour is not acceptable. I will be polite at all times.
12. **Friends on Social Networking Sites**. School staff (using personal profiles) and students (excepting family members, at your own risk) should not be friends on social networking websites.
13. **Commercial activities.** I will not engage in any commercial activities for personal financial gain, political purposes or advertising.
14. **Disrepute**. I will not bring the school into disrepute or risk of litigation.

I realise that any contravention of the rules set out in this document may result in a disciplinary procedure. If I break any of these rules then my use of ICT in school may be limited or completely stopped. My activities may also be reported to other people.

Where necessary a Police Officer may confiscate a device and/or speak to a student about the content on the device.